

12-2020

Politeness in security directives: Insights in browser compliance for the human element

Deanna House
University of Nebraska at Omaha

Gabe Giordano
Ohio University

Follow this and additional works at: <https://digitalcommons.unomaha.edu/isqafacpub>



Part of the [Information Security Commons](#)

Recommended Citation

House, Deanna and Giordano, Gabe, "Politeness in security directives: Insights in browser compliance for the human element" (2020). *Information Systems and Quantitative Analysis Faculty Publications*. 106.
<https://digitalcommons.unomaha.edu/isqafacpub/106>

This Article is brought to you for free and open access by the Department of Information Systems and Quantitative Analysis at DigitalCommons@UNO. It has been accepted for inclusion in Information Systems and Quantitative Analysis Faculty Publications by an authorized administrator of DigitalCommons@UNO. For more information, please contact unodigitalcommons@unomaha.edu.

Politeness in security directives: Insights in browser compliance for the human element

Deanna House (University of Nebraska at Omaha, United States), Gabe Giordano (Ohio University, United States)

<https://doi.org/10.1016/j.cose.2020.102007>

Abstract

The technical protection provided by information security technology is necessary as a frontline defense against threats. However, the human element adds great risk to systems and cannot be ignored. This research explores the human elements related to security communications and intention to comply with security directives. Security communications are more-commonly being sent using richer computer-based channels. While the goal of security communications is the gain compliance, there is still much to learn related to what influences a user to comply. This research explores the effects that (im)politeness has on intention to comply with security directives. The research utilized an experiment that focused on secure browser setting directives using several types of online communication. The subjects were randomly assigned to receive communications/directives that were text-based, text/image-based, or video-based. The communications were also grouped into polite and impolite messaging. The results for the overall model indicated perceived richness had a negative influence on perceived mental workload. Additionally, perceived mental workload resulted in a decreased intention to comply with security directives. There were no significant differences between polite and impolite groups for the treatment groups with text-based and text/image-based messaging. However, in the video-based treatment, the relationship between perceived richness and intention to comply with security directives was significantly different between the polite and impolite groups.

Keywords

Politeness theory

Media richness

Mental workload

Secure browser settings

Security compliance

Human element

Experiment

1. Introduction

Information security continues to gain in technical advances to protect users and organizations from adversaries. Technical protective measures are necessary as front line protection ([Conkle, 2020](#)). Tactics developed by adversaries are frequently set up to bypass even the most sophisticated security technology and instead target the human element ([The One Brief, 2020](#)). As mentioned in a study by McAfee that collected data from information technology and information security professionals representing 1155 organizations across the globe, poor user security practices are still one of the top threats to organizations ([McAfee, 2017](#)).

Politeness has been well-explored in communications literature yet also crosses many research disciplines ([Watts et al., 1992](#)). However, little research has been conducted related to politeness in information systems; specifically politeness in security messages and directives. The increase of online computing systems and associated services have placed importance on computer security and secure computing behavior. IT professionals and researchers now recognize that one of the biggest threats to computer security is at the user level, due to the fact that most users do not take appropriate proactive measures to improve their computer security practices. Default Internet browser settings can leave a user vulnerable. Default settings are not frequently changed by computer users which is challenging considering that browser based threats remain an issue ([Matteson, 2018](#)). Unfortunately, very few easy-to-implement methods to improve user security behavior have been identified.

Another important computing trend is the movement of communication towards new computer-based channels. There is a continual movement of communication in general to email; however, we also now see communication moving to channels like synchronous chat and full audio-visual channels. More frequently, security-related communications in organizations are being sent over these newer computer-based communication channels ([Park, 2008](#); [Haber, 2009](#)) including audio, streaming and other mechanisms that are high in information richness ([Shaw et al., 2009](#)). Security communications are purposeful in that the goal of the communication is often to gain compliance of the reader ([Vergaro, 2002](#)). Since it is important that communications related to

information security are not ignored by individuals within an organization, it is necessary that the communication channel fit the task ([Daft et al., 1987](#)).

This research explores the effect that politeness has across multiple types of media instructions related to securing a web browser by changing its settings on a webpage. “Motivation for politeness stems from desire to maintain social equilibrium between the interactants and to present and have confirmed an identity that allows the exercise of power without endangering the social fabric” ([Locher, 2004](#), pg. 59). Politeness is seen as a precondition to human cooperation and can invoke a need to maintain common ground; even among strangers (such as a computer). One of the communication practices that has been investigated in more traditional communication settings when investigating the effectiveness of directive-related communications is the impact of politeness. Politeness has a significant influence in traditional communication settings such as face-to-face and phone, however it has not been investigated in newer computer-based communication settings - in a computer-security-directive context. This study seeks to gain an understanding of the effectiveness that politeness can have on intention to comply with computer-security requests over new communication channels.

2. Literature review and hypotheses development

2.1. Compliance

“Compliance refers to a particular kind of response – acquiescence - to a particular kind of communication – a request” (pg. 592). Compliance has been studied in many contexts, such as directives related to medical recommendations ([Rissman and Rissman, 1987](#)); environmental issues ([Pelletier and Sharp, 2008](#)); emergency notifications ([Han et al., 2015](#)); protective strategies ([Johnston et al., 2015](#)); and information security policies ([Puhakainen and Siponen, 2010](#); [Cram et al., 2019](#); [Moody et al., 2018](#)). Specific instructions, such as those that would be present in message directives, can lead to an improvement in performance and/or compliance ([Boussalis et al., 2018](#)). Subjects that have are provided with a choice are more compliant ([Heilman and Garner, 1975](#)). It is possible that the threat of having unsafe browser settings can create a sense of discomfort for individuals. The compliance would alleviate that discomfort.

2.2. Mental workload

Mental workload is defined as the difference between task performer capabilities and demand of the task ([Jex, 1988](#)). It reflects the amount of “cognitive capacity” necessary to complete a task ([O'Donnell and Eggemeier, 1986](#)). There is a mental price that exists when accomplishing a task – referred to as a mental workload ([Hart and Wickens, 1990](#)). A person has a limited capacity when performing a task. When that capacity is exceeded it can cause overload which in turn affects task performance ([O'Donnell and Eggemeier, 1986](#)). Additionally, workloads are “experienced as a natural consequence of many daily activities” (Hart & Straveland, pg. 141). Mental workload has been studied in a variety of contexts including driving ([Morgan and Hancock, 2011](#); [Hoogendoorn et al., 2012](#)); computing ([Mayer and Moreno, 1988](#); [Wästlund et al., 2008](#); [Wiebe et al., 2010](#); [Di Stasi et al., 2013](#)) and smart phones ([Iyengar and Florez-Arango, 2013](#)).

2.3. Media richness

A first important element of online communication is the fit of the communication media used to the task. Different media have differing abilities to transmit rich messages. Information richness can be explained as the “ability of information to change understanding within a time interval” ([Daft and Lengel, 1986](#), pg. 560). Media richness is the ability of a medium to transmit rich messages due to the availability of elements such as social cues, language variety, and personal focus ([Lee et al., 2007](#); [Daft et al., 1987](#)). [Daft et al., \(1987\)](#) contributed a hierarchical scale for media richness with communication channels such as face-to-face on the high end of the media richness spectrum and standard reports/unaddressed documents on the low end of the media richness spectrum.

It is important that the correct pairing of media richness and message occur in order for individuals to give their full attention to a message, not have negative side effects from interpreting a communication, and for a communication to be successful ([Trevino et al., 1990](#)). Media Richness Theory suggests that rich messages should be used for more complex, non-routine messages ([Aliu et al., 2017](#)). These types of messages often contain elements of time pressure, do not contain all the foundational understanding needed by receivers, do not have a common frame of reference between sender/receiver, and are misinterpreted ([Lengel and Daft, 1988](#)). Computer security-related communications can be seen as non-routine, as these

communications are providing instructions to the recipients without personalized/relationship-specific details, and because they come at unexpected times.

Rich media are a good fit for these types of communications because they support higher information processing ([Maity et al., 2018](#)). Specific to information security, comprehension of security awareness has been found to be higher for learners when materials are presented in a richer format such as video with sound, text, and pictures ([Shaw et al., 2009](#)). Lower comprehension from lean media (such as text) leads to more unclear information, which in turn increases the mental workload for individuals and can even lead to an information overload ([Schick et al., 1990](#); [Schneider, 1987](#)). In addition, less rich communications, such as text-based communications, can be more difficult than richer forms ([Carnevale and Probst, 1997](#)). The use of richer technology, such as video, has been found to have a decrease in workload ([Iyengar and Florez-Arango, 2013](#)).

Security communications are also often directive - they guide a message recipient to perform an act ([Miller et al., 2008](#)). Rich messages are also hypothesized to be a better fit for directive-based messages ([Lee et al., 2007](#)). Much of this is likely due to social presence theory, which explains how cues and the perceived distance between communicators can lead to a feeling of realness (or social richness) which affects receivers' behavior. Lean communications have low social presence, which can cause individuals to pay less attention to messages and group norms ([Short et al., 1976](#); [Sproull and Kiesler, 1986](#)). Previous research has shown that individuals in a low social presence group setting are less likely to make decisions and judgments ([Giordano et al., 2011](#)). Therefore, directives in richer messages, which have a higher level of social presence, should be taken more seriously by receivers.

We predict the following:

Hypothesis 1: Security directives perceived as richer will have a decreased perceived mental workload.

Hypothesis 2: Security directives perceived as richer will have an increased security directive compliance intention.

2.4. Mental workload and compliance

Studies related to cognitive load and media richness have explored how the increased mental workload can negatively affect information processing ([Badger et al., 2014](#)). This can also affect performance negatively and result in increased errors ([Yan et al., 2019](#)). From a technology perspective, there is a relationship between workload and unfavorable views which can result in the avoidance of the task ([Iyengar and Florez-Arango, 2013](#)). In addition, increased mental workload has been shown to affect task performance ([Hsu et al., 2015](#)). This divergence of mental workload and task performance can be resolved by a reduction in compliance ([Hoogendoorn et al., 2012](#)). As found by [Dixon and Wickens \(2006\)](#), compliance degrades in situations that entails a high mental workload. Mental workload as a task characteristic was manipulated through the tasks that the users were performing, which was not collected directly. Similar to [Kokini et al. \(2012\)](#), the users' subjective perception of mental workload was measured, defined as perceived mental workload. Thus, we predict the following:

Hypothesis 3: A higher level of perceived mental workload will have a decreased security directive compliance intention.

2.5. Competence, goodwill, trustworthiness - credibility

Credibility as an application area explores how people process and evaluate information ([Rieh and Danielson, 2008](#)). A message that is seen as credible can have persuasive properties on its recipient ([McGinnies, 1973](#); [Sterthal et al., 1978](#)). Previous research related to credibility has explored the three factors of competence, goodwill, and trustworthiness ([McCroskey and Teven, 1999](#)). Competence is seen as a key component when determining message quality and trustworthiness of the source ([Paglieri et al., 2014](#)). Goodwill is associated with a source's perceived level of caring ([Teven and McCroskey, 1997](#); [Teven, 2008](#)). Trustworthiness can be viewed as having character, honesty, and a general genuineness ([McCroskey and Teven, 1999](#)). Communications from untrustworthy sources can have an initial period of resistance ([Hovland and Weiss, 1951](#)). Additionally, competence, goodwill, and trustworthiness have been shown to correlate positively with learning and positive feelings towards the instructor ([Teven and McCroskey, 1997](#)). Lastly, computer-based communications are seen as more credible and result in an increased level of compliance when credibility is high ([Jiang et al., 2000](#)). Related to richer communications, it has been determined that the richer information sources can convey more information and thus be considered more credible ([Cable and Yu, 2006](#)). When information

richness is high, the influence on credibility will also be high ([Levy and Gvili, 2015](#); [Hung et al., 2011](#); [Yang et al., 2012](#)). Thus, hypothesis 4 and hypothesis 5 are below.

Hypothesis 4: A credible communication will have an increased security directive compliance intention.

Hypothesis 5: Security directives perceived as richer will have a positive influence on credibility.

2.6. Politeness

Politeness theory can help understand different styles of communication and how to communicate effectively ([Goldsmith, 2007](#)). Politeness has been studied in research related to communication by a variety of researchers in multiple contexts such as student team emails ([Lam, 2011](#)); relationship dynamics ([Dillard et al., 1997](#)); resistance to persuasion ([Jenkins and Dragojevic, 2011](#)); workplace friendships ([Sias et al., 2012](#)); and e-mail ([Jessmer and Anderson, 2001](#)). Politeness has multiple research perspectives which are discussed in detail below.

[Leech's Politeness Principle \(1983\)](#) and revised (2014) suggests that interactions are generally preferred polite rather than impolite. This includes the minimization of unfavorable expressions and maximization of favorable expressions ([Fraser, 1990](#)). There is an avoidance of communicative discord which means a sharing of incompatible goals ([Leech 2014](#)). Brown and Levinson's Politeness Theory ([Brown and Levinson, 1987](#)) focuses on the *face-saving viewpoint*. The concept of face can be defined as a self-claimed positive social value ([Goffman, 1967](#)). It can also be explained as the image a person gives him/herself during an interaction ([Locher, 2004](#)). Threats to face can be positive (which entails the desire for approval) or negative (which entails a desire not to be imposed on) ([Goldsmith, 2007](#)). Politeness is broken down into three main strategies: 1) positive, 2) negative, and 3) off-record ([Brown and Levinson, 1987](#)). Positive politeness is the “positive self-image” one has for oneself while negative politeness is more avoidance-based and focuses on “self-determination” ([Brown and Levinson, 1987](#), pg. 70).

Overall, the purpose of politeness is “to consider others’ feelings, establish views of mutual comfort, and promote rapport ([Hill et al., 1986](#), pg. 349). In the English-speaking world,

politeness can relate back to social norms; that positive/polite occurs when an action is in line with a norm and negative/impolite occurs when it is not ([Fraser, 1990](#)). [Watts \(2003\)](#) takes a more flexible approach and discusses a model which would look at the individual's interpretation of '(im)polite' language. He proposes two concepts: politic behavior (language beyond what is expected) and linguistic politeness (language beyond politic behavior) ([Watts, 2003](#)).

Impoliteness, being the opposite of politeness, is best studied by building on politeness theory ([Leech, 2014](#)). Impoliteness is defined as "behavior that is face-aggravating in a particular context" ([Locher and Bousfield \(2008\)](#), pg. 3) and focuses on discord ([Leech, 2014](#)).

Impoliteness has also been clarified as a communication that delivers intentional aggression/offense to the message recipient ([Bousfield 2008](#)). Impoliteness involves "taking value from the other person and giving value to oneself" ([Leech, 2014](#), pg. 222). In the case of an information security request, the computer is undermining the user to make a command.

Impoliteness can be seen as a discord with an expected behavior in a specific context ([Culpeper, 2011](#)). Research by [Carlo & Yoo \(2007\)](#) found that negative politeness was more frequently used online (versus face-to-face). This is concerning, considering impolite systems or communications can result in users ignoring messages ([Whitworth, 2005](#)). Additionally, speech acts that are more direct can be deemed impolite ([Brown and Levinson, 1987](#); [Leech, 1983](#); [Stephan et al., 2010](#)) yet if there is a social relationship between parties direct speech is allowed and considered polite ([Dillard et al., 1997](#)). It is interesting given that a computer is not a human, yet social rules such as politeness are applied ([Nass et al., 1999](#); [Whitworth, 2003](#)).

Politeness and technical communications have been studied related to written communications ([Cherry, 1998](#); [Graham and David, 1996](#); [Hagge and Kostelnick, 1989](#); [Myers, 1991](#); [Riley, 2003](#)); e-mails and instant messaging ([Brennan and Ohaeri, 1999](#); [Burke and Kraut, 2008](#); [Dubrovsky et al., 1991](#); [Kiesler and Sproull, 1992](#); [Lowry et al., 2006](#); [Rogers and Lee-Wong, 2003](#); [Vinagre, 2008](#)), and spoken communication ([Moore, 1992](#), [Mackiewicz, 2004](#); [Mackiewicz and Riley, 2003](#); [Riley and Mackiewicz 2003](#); [Friess 2011](#)). Generally, politeness is seen as a mechanism to promote acceptance ([Moore, 1992](#)). This is of particular importance when there is not already a common perspective in place ([Daft et al., 1987](#)) as would be the case in the communication of browser security amongst computer users. It is expected that a directive perceived as more polite will generally result in a higher compliance rate ([Miller et al., 2008](#)) and potentially a politeness bias ([Lee et al., 2019](#)).

Overall, we expect that polite communications will moderate each of the relationships previously discussed, due to the fact that polite communications are seen as more understanding, accepting, and team-based.

Hypothesis 6: The group that receives polite communications will be statistically different from the group that receives impolite communications.

○ *Polite Communication will enhance the effect from H1: Security directives perceived as richer will have a decreased perceived mental workload.*

○ *Polite Communication will enhance the effect from H2: Security directives perceived as richer will have an increased security directive compliance intention.*

○ *Polite Communication will enhance the effect from H3: A higher level of perceived mental workload will have a decreased security directive compliance intention.*

○ *Polite Communication will enhance the effect from H4: A credible communication will have an increased security directive compliance intention.*

○ *Polite Communication will enhance the effect from H5: Security directives perceived as richer will have a positive influence on credibility.*

2.7. Methodology

The data was collected in a lab setting in a large Midwestern university. The subjects were students in the College of Business and participation was voluntary. The participants were not given course credit for participation, but they were entered in a drawing to win 1 of 4 \$25 Amazon gift cards. 224 subjects agreed to participate in the study. As part of the informed consent process, participants were told that they were participating in research related to “Internet Safety Through Browser Settings” and that they would be performing tasks related to browser security. In order to keep consistency in the language communicated about the study, the same experimental procedures were used (shown in [Appendix A](#)).

The data was collected using a 2×3 (polite/impolite X text/image/video) experiment website that the subjects accessed from a url link provided by the researcher. The treatments were randomly assigned to subjects. In order to keep consistency in the experiment, all participants were handed headphones and instructed to turn on the sound on their computers. Only the treatments with video media had sound. The url took the participants to websites that had

different content based on the assigned url. The wording of the impolite and polite treatments were worded appropriately based on prior research. The politeness treatment utilized strategies to convey solidarity ([Brown and Levinson, 1987](#); [Park 2008](#)): Politeness could include the use of downgraders such as possibly and please ([Lam, 2011](#)); supportive moves that soften the force of a message (acknowledging discomfort) ([Lam, 2011](#)); assert common ground ([Brown and Levinson, 1987](#)); Gratitude (appreciate) ([Danescu-Niculescu-Mizil et al., 2013](#)); Deference (good work) ([Danescu-Niculescu-Mizil et al., 2013](#)); Indirect (by the way)([Danescu-Niculescu-Mizil et al., 2013](#)).

The impolite treatment was conveyed by impoliteness or negative politeness that may cause loss of face: use of second-person personal pronoun, “you” ([Zhang, 2013](#); [Ali, 2009](#)); second-person pronoun start ([Danescu-Niculescu-Mizil et al., 2013](#)); aggravating moves such as threatening reprimand ([Lam, 2011](#); [Jessmer and Anderson, 2001](#)); direct levels of speech such as performing something forcefully([Lam, 2011](#)); using an insisting adverb (must) ([Gupta et al., 2007](#)); factuality (in fact) ([Danescu-Niculescu-Mizil et al., 2013](#)); Direct start (so) ([Danescu-Niculescu-Mizil et al., 2013](#)). Lastly, the text was checked using the computational politeness app, located at <http://politeness.cornell.edu.leo.lib.unomaha.edu/> and discussed in [Danescu-Niculescu-Mizil et al., 2013](#). All of the impolite and polite treatment wordings scored as was expected (impolite for the impolite treatments/instructions and polite for the polite treatments/instructions). The media treatments were text, which contained instructions with text only. The text-image treatment contained text with accompanying image instructions showing subjects how to find the appropriate browser menu/setting. Lastly, the video media treatment contained a video that was recorded prior to the experiment and placed on YouTube (www.youtube.com). The video had sound/voice instructions along with a record of the steps that the subject was performing.

The website content was created by conducting a research review for recommended secure browser settings from the top three Internet browsers: Google Chrome, Mozilla Firefox, and Microsoft Internet Explorer. In the experiment, the participants were instructed to use Internet Explorer as this was the recommended browser for the college of business. The participants performed three steps to secure their browsers, changing the security zone, using activex filtering, and using smartscreen filters. Examples of the polite/text based site and the impolite/text with images site are shown in [Appendix B](#).

Immediately after the subjects completed the experiment, they completed a survey. The survey items were adapted from existing scales. The Hart & Straveland ([1988](#)) NASA-TLX instrument is one of the most widely used measurement instruments for perceived mental workload ([Wiebe et al., 2010](#)). The use of a multi-dimensional workload was developed by [Hart and Straveland \(1988\)](#) to help reduce problems with between-subject variability in a subjective scale. The other constructs were measured using: security directive compliance intention ([Herath and Rao, 2009](#)); perceived richness ([Carlson and Zmud, 1999](#)); and credibility which consists of goodwill, trustworthiness, and competence ([McCroskey and Teven, 1999](#)). As there were several data collections that occurred over several weeks, the subjects were asked not to discuss any details related to the study with others either in the class or in other classes. After the data collection was completed, the subjects were debriefed about the study.

2.8. Analysis and insights

The survey items for perceived mental workload, perceived richness, and security directive compliance intention are reflective indicators and credibility is a formative indicator as defined by [Petter et al., 2007](#). The constructs were checked for validity and reliability in SPSS. [Table 1](#) displays the Cronbach's alpha, reliability, AVE, and square root of the AVE on the diagonals for the constructs. In order to ensure internal consistency, it is suggested by [Hair et al. \(2010\)](#) that several item measures are used. The item measures can be viewed in [Appendix C](#). Perceived mental workload had a Cronbach's alpha of .585. Cronbach's alpha of $< .7$ (but not less than .6) is considered acceptable in exploratory research ([Hair et al. 2010](#)). Thus, item PW4 was dropped, which improved the reliability to .865. The model was run in Smart PLS 3.0 ([Ringle et al., 2015](#)). An invariance test was run to test for measurement invariance. All items were greater than .05 which indicates that there are no issues with measurement invariance and compositional invariance is established. The correlation matrix was checked ([Table 1](#) below).

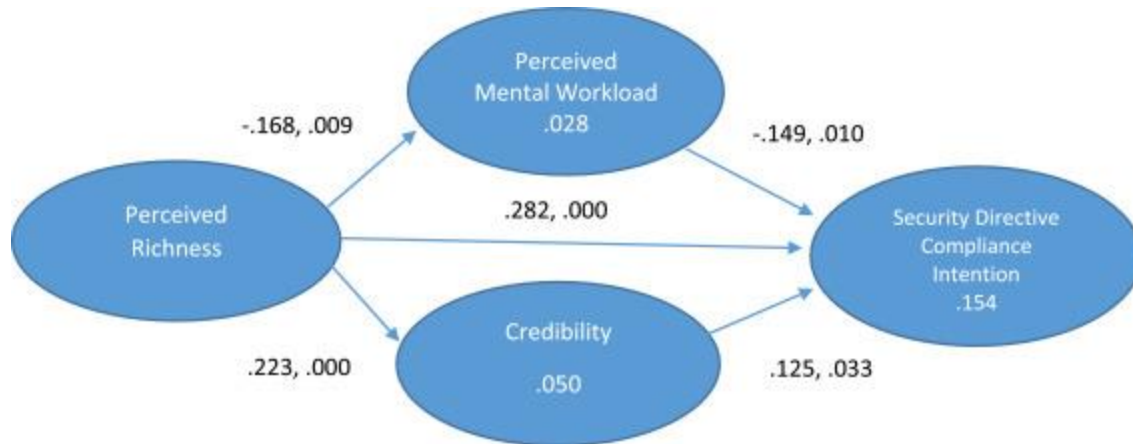
Table 1. Composite Reliability, Cronbach's Alpha, AVE, Correlation Matrix, and Square Root AVE

	Composite Reliability	Cronbach's Alpha	AVE			
Perceived Media Richness	.792	.658	.5	.703		
Perceived Mental Workload	.902	.865	.65	-	.806	
Security Directive Compliance Intention	.64	.885	.79	-	.205	.887
Credibility*	.95	.948	.523	-	.280	.219 .723
				.206		

*formative

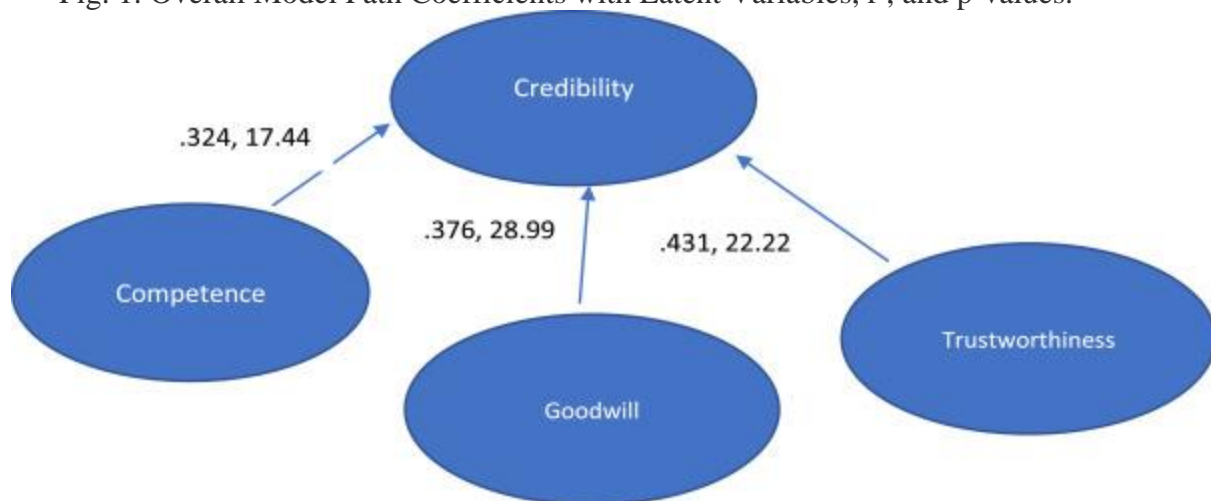
Composite reliability was good and within the recommended .7 or greater for all variables with the exception of security directive compliance intention. The composite reliability for security directive compliance intention was .64 which is considered within an acceptable range for exploratory research ([Bagozzi and Yi, 1988](#)); with values less than .6 indicating a lack of reliability ([Hair et al., 2011](#)). The AVEs all exceeded the recommended threshold of .50 or greater ([Hair et al., 2010](#)) which indicate that convergent validity is acceptable. It was stated by [Fornell and Larcker \(1981\)](#) that convergent validity is acceptable with AVEs less than .5 provided that composite reliability is greater than .6. There are no other indicators of issues with convergent validity so the authors proceeded with the exploratory factor analysis. An exploratory factor analysis was conducted using SPSS for the three reflective factors, perceived mental workload, perceived richness, and intention to comply with security directives. The Kaiser-Meyer-Okin measure of sampling adequacy was .795 which is above the recommended .6 ([Kaiser, 1974](#); [Cerny and Kaiser, 1977](#)). The initial scree plot (performed with principal components extraction) indicated that there were 3 factors which provided the value for the next test within the exploratory factor analysis. A promax rotation was first performed, to verify that there were no correlation issues. All three factors loaded properly within the expected constructs with no correlation issues. A varimax rotation was performed next, also with no issues or cross loadings. In order to take the formative variable into consideration, we re-ran the exploratory factor analysis with credibility. The Kaiser-Meyer-Okin measure of sampling adequacy was .899 and there were 6 factors that loaded, with some cross-loadings across the different formative constructs within credibility (which would be expected).

Multigroup Analysis was utilized for the pre-defined groups ([Sarstedt et al., 2011](#)) polite (impolite, polite) and richness (text, image/text, video). The variable *credibility* is a formative factor as determined by [McCroskey and Teven, 1999](#). Therefore, the analysis was run with credibility as a second order factor. Latent variable scores by running the model with the second order factors, then the model was re-run using the latent variable scores. The results are shown in [Fig. 1](#), [Fig. 2](#), and [Table 2](#) below.



1. Download : Download high-res image (273KB)
2. Download : Download full-size image

Fig. 1. Overall Model Path Coefficients with Latent Variables, r^2 , and p-values.



1. Download : Download high-res image (235KB)
2. Download : Download full-size image

Fig. 2. First Order Formative Path Coefficients and T Statistics

Table 2. Path Coefficients, T statistics and p-values, overall model

	Path Coefficients	T Statistics (O/STDEV)	P Values (1-tailed)
H1: Perceived Richness -> Perceived Mental Workload	-.168	2.359	0.009
H2: Perceived Richness -> Security Directive Compliance Intention	.282	3.645	0.000
H3: Perceived Mental Workload -> Security Directive Compliance Intention	-.149	2.354	0.010
H4: Credibility -> Security Directive Compliance Intention	.125	1.837	0.033
H5: Perceived Richness -> Credibility	.223	3.503	0.000

Table 3. p-values for group differences across media (non-parametric group differences)

	p-Value Impolite vs. Polite Text	p-Value Impolite vs. Polite Image	p-Value Impolite vs. Polite Video
Perceived Richness -> Perceived Mental Workload	.101	.382	.298
Perceived Richness -> Intention to Comply	.972	.501	.043
Perceived Mental Workload -> Security Directive Compliance Intention	.528	.282	.095
Credibility ->			
Security Directive Compliance Intention	.760	.592	.176
Perceived Richness -> Credibility	.081	.621	.053

The overall model was supported. H1, security directives perceived as richer will have a decreased perceived mental workload was supported ($\beta=-.168$, $t=2.359$, $p\text{-value}=.009$). H2 was also supported, with richer security directives having in increased influence on intention to comply with security directives ($\beta=.282$, $t=3.645$, $p\text{-value}=0$). Perceived mental workload also had a significant relationship with intention to comply with security directives, when perceived mental workload was perceived as high, individuals had a decreased intention to comply with security directives ($\beta=-.149$, $t=2.354$, $p\text{-value}=.010$) providing support for H3. The relationship

was as predicted between credibility and intention to comply with security directives was significant, providing support for H4 ($\beta=.125$, $t=1.837$, $p\text{-value}=.033$). The relationship between perceived richness and credibility was significant, which provides support for H5 ($\beta=.223$, $t=3.503$, $p\text{-value}=0$). [Fig. 2](#) shows the path coefficients and T-Statistics for the first order formative constructs for credibility, competence, goodwill, and trustworthiness.

To test H6, group differences between polite and impolite, a Multi-group analysis (MGA) was run in SmartPLS 3. The use of MGA provides the opportunity to explore differences amongst groups and in the case of this research differences amongst treatments. The PLS-MGA test was utilized, which is a non-parametric significance test ([Henseler et al., 2009](#)). The results were mixed, as there was not a significant difference between groups in the overall model. However, when exploring the model between groups with media type, some of the relationships were significantly different across groups. For example, there were no significant differences across text-based messages or messages with text and image, but video messages did show a significant difference. The relationship between perceived richness and intention to comply with security directives was significant ($p\text{-value}=.043$). The relationship between perceived richness and credibility had a weak relationship ($p\text{-value}=.053$) but was not significant.

3. Discussion

This research explored the group differences of politeness (or lack thereof) related to media richness, perceived mental workload, and credibility on the intention to comply with security directives. While the groups assigned treatments that were leaner on the media richness scale (text, text/image) did not have significant differences in polite/impolite communications, there was a statistically significant group difference in the relationship between perceived richness and intention to comply with security directives. This finding is interesting due to the fact that richer communications (such as video) that are perceived as polite could have an influence on compliance related to security directives. This relates to research performed by Heilman & Garner ([Heilman and Garner, 1975](#)) which found that compliance could be influenced in a positive manner when the blow of a threat was softened by boosting positive feelings. However, when feelings of autonomy were threatened, such as those that exist in negative face aspects of politeness, compliance could be lacking and result in defiance. Also, as found by [Jenkins and Dragojevic \(2011\)](#), messages that used forceful language can result in a greater perception of

threat to face. Thus, research supports these findings that the groups would be statistically different. Security training and awareness frequently utilize video as a method of informing users of secure behaviors ([Haber, 2009](#)). The use of videos and improved comprehension has been studied ([Shaw et al., 2009](#)) but further study on the compliance after the initial training has occurred is needed. This study helps explore if politeness could be an influential factor.

Lack of awareness ([Adams and Sasse, 1999](#)) and lack of technical expertise ([Shropshire et al, 2010](#)) can affect secure behaviors. Developing effective training solutions is important when taking a user's everyday usage into consideration. Security behavior during browsing can be a challenge to most users. Generally, users are focused on the task that they are completing online, not security indicators ([Alsharnouby et al, 2015](#)). Therefore it is imperative to practice secure browsing behaviors. However, users are constantly being pushed information which makes it difficult to determine which tasks will ensure secure browsing behavior. In addition, there is a struggle with users to balance the need for control with the view that computers provide the directives and are the most knowledgeable ([Whitworth, 2005](#)). Directives are intended speech acts that are expected to produce a behavior ([Jenkins and Dragojevic, 2011](#)). The struggle of power with an underlying threat of a sanction can be detrimental to communication and result in self-preservation ([Moore, 1992](#)). In addition, communication that is online does not have social cues ([Sproull and Kiesler, 1986](#)). Therefore, it is important that politeness be used for the overall good of the user to result in secure browser behaviors.

The research has several limitations which will be discussed below.

4. Limitations

The study was conducted over a period of two weeks. While the researchers did their best to ensure that the research steps were consistent (see [Appendix A](#)) and emphasized confidentiality to the subjects, it is possible that subjects that performed the tasks early on in the data collection period discussed the study with subjects that performed the tasks later on. While the authors made every attempt to address any issues that could be created by selection bias, the subjects were students at a university. In addition, the subjects were mostly in the age group 18-24. While this can be considered a limitation, the study explored compliance related to securing an Internet browser. For the scope of the study, current users of Internet browsers were targeted. The age

group, while younger, had exposure to using Internet browsers as this study was conducted in a university setting in a lab.

While there were some differences noted between the impolite and polite groups, particularly the video treatment, in the text and image treatments the relationships were not significantly different between groups. This could be explained by the fact that text and images (with text) may have been more difficult for subjects to discern the difference between text that was polite and text that was impolite. [Jessmer and Anderson \(2001\)](#) found that polite messages were seen as more positive and also as written by a more friendly person. However, as mentioned by [Dynel \(2015\)](#) impoliteness has many different nuances and subtypes. Implications for research, implications for practice and conclusions follow.

5. Implications for research

This research has some important findings that contribute to the field. Related to communication style, the level of politeness paired with the media type are important for security directive compliance. Researchers should consider human driven characteristics of communication (such as politeness), as well as media influenced characteristics (such as richness) when investigating security messages. Other communication choices that display empathy (such as options for how to view a security training message) should also be investigated in future research about security communications. Additional research could look at motivations behind polite communications versus impolite. Communication that is asynchronous has different requirements over face-to-face communications, with social distance having a significant effect on communication strategies rather than power distance in the case of face-to-face ([Vinagre, 2008](#)). Some of these strategies include claiming common ground ([Vinagre, 2008](#)) which could be influential in the case of other communication situations in which politeness is important. For example, politeness in phishing emails, a significant source of business email compromise (BEC) in organizations, may be more persuasive to the message recipient. Research has also been conducted related to motivation in the workplace and credibility ([Holmes and Parker, 2017](#)) and media richness among communications between employees and managers ([Armengol et al., 2017](#)). Extending this research to include politeness strategies in the workplace related to information security compliance would be useful for further development and improvement related to information security training and awareness.

6. Implications for practice

As mentioned in the introduction, the human element is necessary for securing systems. This includes Internet browser settings, as default settings can leave a user vulnerable to malware, viruses, and privacy exploits. These vulnerabilities affect users at home and in the workplace. Related to media selection, richness and social presence matter in a security directive setting. Extra care and consideration in the development of security directives so that they are richer communications can have an impact on compliance.

As has been found true in other settings, media richness affects how people perceive the complexity (difficulty) of security actions and their likelihood to take action. So, rich media should be used as much as possible. Rich messages can be more work to create, so if they aren't directed to use this type of messaging, many individuals might choose not to do this by default. It is also important is how a message is crafted within a medium. In time-pressured, high risk settings we often default to direct, matter-of-fact directives that do not show empathy in a style that is typically perceived as impolite. While there have been mixed results on messages related to politeness and computer-mediated communications, our research provides evidence that politeness does in fact influence compliance in richer communications.

7. Conclusion

This research provided insights related to the influence that politeness and richness of media can have on security directive compliance intention. Computer users are frequently given directives for remaining secure. Richer communications have been shown to have a higher perception of the amount of information ([Frasca and Edwards, 2017](#)) which could lead to better comprehension and compliance. Security directives that intend to provide recommendations for improving security, such as on an Internet browser can have an unintended perception of impoliteness or forcefulness. According to research by [Lam \(2011\)](#), direct speech acts can be more effective when paired with downgrader text (such as *please* and *possibly*) that have the intention of lessening the force of a message. These elements of politeness were shown as influencers in our research. Additionally, the use of videos for communicating security directives can be a useful option, particularly when complicated tasks are given. This research is an important stepping stone to determining factors that influence compliance in the human element so that information systems are better protected.

CRedit authorship contribution statement

Deanna House: Funding acquisition, Investigation, Resources, Software, Writing - review & editing, Data curation, Formal analysis, Project administration, Visualization, Writing - original draft.

Gabe Giordano: Conceptualization, Methodology, Supervision, Validation, Funding acquisition, Investigation, Resources, Software, Writing - review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

An earlier version of this manuscript was presented at the 11th edition of the annual Dewald Roode Workshop on Information Systems Security Research, held in Louisiana, USA and hosted by Professor Tom Stafford of Louisiana Tech University, who was also the Guest Editor for this special issue. The annual workshop is sponsored by the IFIP Working Group on Information Systems Security Research (8.11/11.13) - <https://ifip-byu-edu.leo.lib.unomaha.edu/> . We thank the workshop participants, anonymous journal reviewers, and Dr. Stafford for their guidance on developing our paper. The authors would also like to thank the Ohio University College of Business and contributors to the EY Research Grant Fund for their support.

Appendix A

Experimental procedures

Good Morning/Afternoon,

We are conducting research on Internet safety through browser settings. We will be handing out informed consent forms for you to sign if you are interested in participating. Your participation is

entirely voluntary, but we appreciate your willingness to contribute to this important research study.

If you are willing to participate, please sign the informed consent. The informed consent provides information about what the study entails. We will keep the signed copy, but we have extra copies if you would like one to take with you.

If you have already participated in this research in another class, please do not participate again.

<<Hand out informed consent>>

A few things about the study before we get started.

Please take out your headphones and unmute the sound on your computers. Please open Internet Explorer. We will be handing out a sheet with a url of a website that you will go to. Please do not leave this site during your participation.

Also, please wait at least 20 seconds on each page to ensure that the entire page is loaded.

Please do not discuss what is on the screen with your classmates.

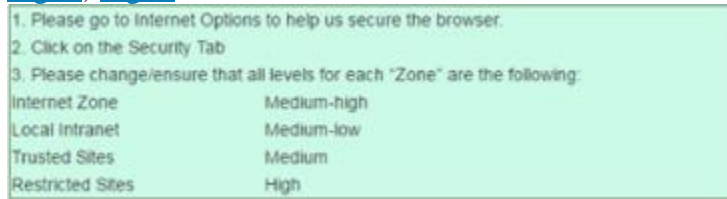
<<Hand out url sheets, they are randomly collated (1-6 treatments) >>

<<After all subjects have completed the study/survey>>

Thank you so much for your participation in this study. For the success of our study, we ask that you do not discuss this study with anyone in this class or any other classes. We will be collecting data for the next 2 – 3 weeks and it is important that you keep your information confidential. Once we have finished the collection of all data, we will return to briefly discuss and debrief you on the purpose of our study.

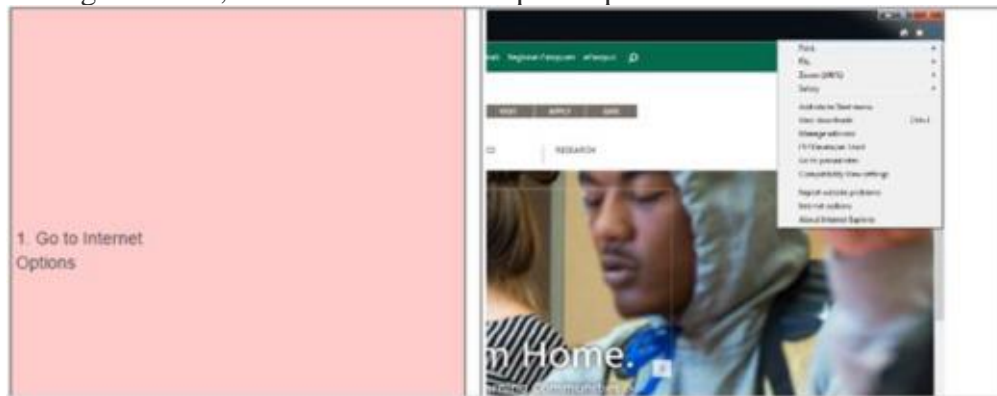
Appendix B Treatment Step Examples

[Fig. 3](#), [Fig. 4](#).



1. Download : Download high-res image (125KB)
2. Download : Download full-size image

Fig. 3. Polite, Text Treatment Example Step.



1. Download : Download high-res image (189KB)
2. Download : Download full-size image

Fig. 4. Impolite, Text with Images Treatment Example Step.

Appendix C Survey Items

The subjects answered the following related to the security steps that they completed. The items were measured as Strongly Disagree to Strongly Agree unless otherwise noted.

Perceived Mental Workload (Hart & Straveland, 1988)	Factor Loadings
How mentally demanding were the security steps?	.886
How physically demanding were the security steps?	.752
How hurried or rushed was the pace of the security steps?	.783
How successful were you in accomplishing what you were asked to do?	—
How hard did you have to work to accomplish your level of performance?	.814
How insecure, discouraged, irritated, stressed, and annoyed were you?	.786
Perceived Richness (Carlson and Zmud, 1999)	

Email allows me to give and receive timely feedback	.532
Email allows me to tailor my message to my own personal requirements.	.648
Email allows me to communicate a variety of different cues (such as emotional tone, attitude, or formality) in my messages.	.781
Email allows me to use rich and varied language in my messages.	.783
Credibility (McCroskey and Teven, 1999) (Measured on a scale of 1 to 7, with the closer the number to the adjective, the more certain the subject is that the message is like that characteristic)	
<i>Competence</i>	
Unintelligent Intelligent	.781
Untrained Trained	.816
Inexpert Expert	.815
Uninformed Informed	.813
Incompetent Competent	.825
Stupid Bright	.750
<i>Goodwill</i>	
Doesn't care about me Cares about me	.788
Doesn't have my interests at heart Has my interests at heart	.874
Self-Centered Not self-centered	.820
Unconcerned with me Concerned with me	.859
Insensitive Sensitive	.819
Not understanding Understanding	.745
<i>Trustworthiness</i>	
Dishonest Honest	.857
Untrustworthy Trustworthy	.860
DishonorableHonorable	.872
Immoral Moral	.864
Unethical Ethical	.888
Phoney Genuine	.889
Security Directive Compliance Intention (Herath and Rao, 2009)	
I am likely to follow organizational security policies	.832
It is possible that I will comply with organizational IS security policies to protect the organization's information systems.	.897
I am certain that I will follow organizational security policies.	.902

References

[Adams and Sasse, 1999](#) A. Adams, M. Sasse

Users are not the enemy

Commun. ACM, 42 (12) (1999), pp. 40-46

[Google Scholar](#)

[Ali, 2009](#) Z. Ali

'Powerless language' for powerful communication: delineating influence in group decision making

Int. J. Learn., 16 (10) (2009), pp. 509-520

[View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Aliu et al., 2017](#) D. Aliu, A. Akatay, A. Aliu

The influence of inter-stakeholders' communication on university-industry collaboration

Sch. Int. J. Bus. Policy Gov., 4 (8) (2017), pp. 78-86

[View Record in Scopus](#) [Google Scholar](#)

[Alsharnouby et al., 2015](#) M. Alsharnouby, F. Alaca, S. Chiasson

Why phishing still works: user strategies for combating phishing attacks

Int. J. Hum.-Comput. Stud., 82 (2015), pp. 69-82

[Article Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Armengol et al., 2017](#) X. Armengol, V. Fernandez, P. Simo, J.M. Sallan

An examination of the effects of self-regulatory focus on the perception of the media richness: the case of e-mail

Int. J. Bus. Commun., 54 (4) (2017), pp. 394-407

[View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Badger et al., 2014](#) J.M. Badger, S.E. Kaminsky, T.S. Behrend

Media richness and information acquisition in internet recruitment

J. Manag. Psychol., 29 (7) (2014), pp. 866-883

[View Record in Scopus](#) [Google Scholar](#)

[Bagozzi and Yi, 1988](#) R.P. Bagozzi, Y. Yi

On the evaluation of structural equation models

J. Acad. Market. Sci., 16 (1) (1988), pp. 74-94

[Google Scholar](#)

[Bousfield, 2008](#) D. Bousfield

Impoliteness in Interaction

John Benjamins Publishing Company, Amsterdam, Netherlands (2008)

[Google Scholar](#)

[Boussalis et al., 2018](#) C. Boussalis, Y. Feldman, H.E. Smith
Experimental analysis of the effect of standards on compliance and performance
Regul. Gov., 12 (2018), pp. 277-298
[View PDF](#)
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Brennan and Ohaeri, 1999](#) S.E. Brennan, J.O. Ohaeri
Why Do Electronic Conversations Seem Less Polite?
The Costs and Benefits of Hedging, Coordination, and Collaboration (WACC 1999), San Francisco, CA (1999)
Paper presented at the International Joint Conference on Work Activities
[Google Scholar](#)

[Brown and Levinson, 1987](#) P. Brown, S.C. Levinson
Politeness: Some Universals in Language Usage
Cambridge University Press, Cambridge, UK (1987)
[Google Scholar](#)

[Burke and Kraut, 2008](#) M. Burke, R. Kraut
Mind Your Ps and Qs: The Impact of Politeness and Rudeness in Online Communities
(2008)
Paper presented at the 2008 ACM Conference on Computer Supported Cooperative Work, San Diego, CA
[Google Scholar](#)

[Cable and Yu, 2006](#) D.M. Cable, K.Y.T. Yu
Managing job seekers' organizational image beliefs: the role of media richness and media credibility
J. Appl. Psychol., 91 (4) (2006), pp. 828-840
[View Record in Scopus](#) [Google Scholar](#)

[Carlo and Yoo, 2007](#) J.L. Carlo, Y. Yoo
"How may i help you? Politeness in computer-mediated and face-to-face library reference transactions
Inf. Org., 17 (4) (2007), pp. 193-231
[Article Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Carlson and Zmud, 1999](#) J.R. Carlson, R.W. Zmud
Channel expansion theory and the experiential nature of media richness perceptions
Acad. Manag. J., 42 (2) (1999), pp. 153-170
[View Record in Scopus](#) [Google Scholar](#)

[Carnevale and Probst, 1997](#) P.J. Carnevale, T.M. Probst
Conflict on the internet

S. Kiesler (Ed.), Culture of the Internet, Lawrence Erlbaum, Hillsdale, NJ (1997), pp. 233-261
[Google Scholar](#)

[Cerny and Kaiser, 1977](#) C.A. Cerny, H.F. Kaiser
A study of a measure of sampling adequacy for factor-analytic correlation matrices
Multivar. Behav. Res., 12 (1) (1977), pp. 43-47
[View PDF](#)
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Cherry, 1998](#) R.D. Cherry
Politeness in written persuasion
J. Pragm., 12 (1) (1998), pp. 63-81
[Google Scholar](#)

[Conkle, 2020](#) T. Conkle
The human element of cybersecurity
Forbes (2020)
Retrieved May 31, 2020 from
<https://www.forbes.com/sites/forbestechcouncil/2020/01/24/the-human-element-of-cybersecurity/#270f22ca3293>
[Google Scholar](#)

[Cram et al., 2019](#) W.A. Cram, J. D'Arcy, J.G. Proudfoot
Seeing the forest and the trees: a meta-analysis of the antecedents to security policy compliance
MIS Q., 43 (2) (2019), pp. 525-554
[View PDF](#)
[CrossRef](#) [Google Scholar](#)

[Culpeper, 2011](#) J. Culpeper
Impoliteness: Using Language to Cause Offence
Cambridge University Press, Cambridge, UK (2011)
[Google Scholar](#)

[Daft and Lengel, 1986](#) R Daft L, R Lengel H
Organizational Information Requirement, Media Richness, and Structural Design.
Manage. Sci., 32 (5) (1986), pp. 554-571
[View PDF](#)
[CrossRef](#) [Google Scholar](#)

[Daft et al., 1987](#) R.L. Daft, R.H. Lengel, L.K. Trevino
Message equivocality, media selection, and manager performance: implications for information systems
MIS Q., 11 (3) (1987), pp. 354-366
[Google Scholar](#)

[Danescu-Niculescu-Mizil et al., 2013](#) C. Danescu-Niculescu-Mizil, M. Sudhof, D. Jurafsky, J. Leskovec, C. Potts
A computational approach to politeness with application to social factors
Proceedings of the ACL, 2013 (2013)
[Google Scholar](#)

[Di Stasi et al., 2013](#) L.L. Di Stasi, A. Antolí, J.J. Cañas
Evaluating mental workload while interacting with computer-generated artificial environments
Entertain. Comput., 4 (2013), pp. 63-69
[Article Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Dillard et al., 1997](#) J.P. Dillard, S.R. Wilson, K.J. Tusing, T.A. Kinney
Politeness judgments in personal relationships
J. Lang. Soc. Psychol., 16 (3) (1997), pp. 297-325
[View Record in Scopus](#) [Google Scholar](#)

[Dixon and Wickens, 2006](#) S.R. Dixon, C.D. Wickens
Automation reliability in unmanned aerial vehicle control: a reliance-compliance model of automation dependence in high workload
Hum. Fact., 48 (3) (2006), pp. 474-486
[View PDF](#)
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Dubrovsky et al., 1991](#) V.J. Dubrovsky, S. Kiesler, B.N. Sethna
The equalization phenomenon: status effects in computer-mediated and face-to-face decision-making groups
Hum.-Comput. Interact., 6 (2) (1991), pp. 119-146
[View PDF](#)
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Dyrel, 2015](#) M. Dyrel
The landscape of impoliteness research
J. Polit. Res., 11 (2) (2015), pp. 329-354
[View Record in Scopus](#) [Google Scholar](#)

[Fornell and Larcker, 1981](#) C. Fornell, D.F. Larcker
“Evaluating structural equation models with unobservable variables and measurement error
J. Market. Res., 18 (1) (1981), pp. 39-50
[Google Scholar](#)

[Frasca and Edwards, 2017](#) K.J. Frasca, M.R. Edwards
Web-based corporate, social, and video recruitment media: effects of media richness and source credibility on organizational attraction
Int. J. Select. Assess., 25 (2017), pp. 125-137

[_View PDF](#)
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Fraser, 1990B](#). Fraser

Perspectives on politeness

J. Pragm., 14 (2) (1990), pp. 219-236

[Article](#) [Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Friess, 2011](#) E. Friess

Politeness, time constraints, and collaboration in decision-making meetings: a case study

Tech. Commun. Q., 20 (2) (2011), pp. 114-138

[_View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Giordano et al., 2011](#) G Giordano, J George, K Marett

Reviewers and the Detection of Deceptive Information in Recorded Interviews

J. Appl. Soc. Psychol., 41 (2) (2011), pp. 252-269

[_View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Goffman, 1967](#) E. Goffman

Interaction Ritual: Essays on Face-to-Face Behavior

Anchor Books, Garden City, NY (1967)

[Google Scholar](#)

[Goldsmith, 2007](#) D.J. Goldsmith

Brown and levinson's politeness theory.

B.B. Whaley, W. Samter (Eds.), Explaining Communication: Contemporary Theories and Exemplars, Lawrence Erlbaum Associates, Publishers, Mahwah, NJ (2007)

[Google Scholar](#)

[Graham and David, 1996](#) M.B. Graham, C. David

Power and politeness: administrative writing in an “organized anarchy”

J. Bus. Tech. Commun., 10 (1) (1996), pp. 5-27

[_View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Gupta et al., 2007](#) S. Gupta, M.A. Walker, D. Romano

A. Paiva, R. Prada, R.W. Picard (Eds.), Springer-Verlag, Berlin, Germany (2007), pp. 203-217

[_View PDF](#)

[CrossRef](#) [View Record in Scopus](#)

[Haber, 2009](#) L. Haber

Security training 101

Netw. World, 26 (16) (2009), pp. 30-33
[View Record in Scopus](#) [Google Scholar](#)

[Hagge and Kostelnick, 1989](#) J. Hagge, C. Kostelnick
Linguistic politeness in professional prose: a discourse analysis of auditors' suggestion letters, with implications for business communication pedagogy
Write. Commun., 6 (3) (1989), pp. 312-393
[View PDF](#)
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Hair et al., 2010](#) J. Hair, Black F., B. Babin, R. Anderson
Multivariate Data Analysis
Prentice Hall, Upper Saddle River, NJ (2010)
[Google Scholar](#)

[Hair et al., 2011](#) J Hair F, C Ringle M, M Sarstedt
PLS-SEM: Indeed a Silver Bullet.
J. Mark. Theory Pract., 19 (2) (2011), pp. 139-152
[Google Scholar](#)

[Han et al., 2015](#) W. Han, S. Ada, R. Sharman, H.R. Rao
Campus emergency notification systems: an examination of factors affecting compliance with alerts
MIS Q., 39 (4) (2015), pp. 909-929
[View PDF](#)
[CrossRef](#) [Google Scholar](#)

[Hart and Staveland, 1988](#) S.G. Hart, L.E. Staveland
Development of NASA-TLX (task load index): results of empirical and theoretical research
P.A. Hancock, N. Meshkati (Eds.), Human Mental Workload, Elsevier Science Publishers B.V, Amsterdam, Netherlands (1988), pp. 139-183
[Article Download PDF](#) [Google Scholar](#)

[Hart and Wickens, 1990](#) S.G. Hart, C.D. Wickens
Workload assessment and prediction
H.R. Booher (Ed.), MANPRINT: An Emerging Technology. Advanced Concepts for Integrating People, Machine, and Organizations, Springer, Dordrecht, Netherlands (1990), pp. 257-296
[View PDF](#)
[CrossRef](#) [Google Scholar](#)

[Heilman and Garner, 1975](#) M.E. Heilman, K.A. Garner
Counteracting the boomerang: the effects of choice on compliance to threats and promises
J. Personal. Soc. Psychol., 31 (5) (1975), pp. 911-917

[_View PDF](#)
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Henseler et al., 2009](#) J. Henseler, C.M. Ringle, R.R. Sinkovics
The use of partial least squares path modeling in international marketing
Adv. Int. Market., 20 (2009), pp. 277-320
[View Record in Scopus](#) [Google Scholar](#)

[Herath and Rao, 2009](#) T. Herath, H.R. Rao
Protection motivation and deterrence: a framework for security policy compliance in organisations
Eur. J. Inf. Syst., 18 (2) (2009), pp. 106-125
[_View PDF](#)
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Hill et al., 1986](#) B. Hill, S. Ide, S. Ikuta, A. Kawasaki, T. Ogino
Universals of linguistic politeness: quantitative evidence from Japanese and American English
J. Pragm., 10 (3) (1986), pp. 347-371
[Article Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Holmes and Parker, 2017](#) W.T. Holmes, M.A. Parker
Communication: empirically testing behavioral integrity and credibility as antecedents for the effective implementation of motivating language
Int. J. Bus. Commun., 54 (1) (2017), pp. 70-82
[_View PDF](#)
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Hoogendoorn et al., 2012](#) R.G. Hoogendoorn, I.M. Harms, S.P. Hoogendoorn, K.A. Brookhuis
Dynamic speed limits: perception, mental workload, and compliance
Transp. Res. Rec.: J. Transp. Res. Board, 2321 (2012), pp. 46-54
[_View PDF](#)
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Hovland and Weiss, 1951](#) C.I. Hovland, W. Weiss
The influence of source credibility on communication effectiveness
Public Opin. Q., 15 (4) (1951), pp. 635-650
[View Record in Scopus](#) [Google Scholar](#)

[Hsu et al., 2015](#) B.W. Hsu, M.J. Wang, C.Y. Chen
Effective indices for monitoring mental workload while performing multiple tasks
Percept. Motor Skills: Learn. Memory, 121 (1) (2015), pp. 94-117
[View Record in Scopus](#) [Google Scholar](#)

[Hung et al., 2011](#) K.H. Hung, S.Y. Li, D.K. Tse

Interpersonal trust and platform credibility in a chinese multi-brand: online community effects on brand variety seeking and time spent

J. Advertis., 40 (3) (2011), pp. 99-112

[View Record in Scopus](#) [Google Scholar](#)

[Iyengar and Florez-Arango, 2013](#) M.S. Iyengar, J.F. Florez-Arango

Decreasing workload among community health workers using interactive, structured, rich-media guidelines on smartphones

Technol. Health Care, 21 (2) (2013), pp. 113-123

[View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Jenkins and Dragojevic, 2011](#) M. Jenkins, M. Dragojevic

Explaining the process of resistance to persuasion: a politeness theory-based approach

Commun. Res., 40 (4) (2011), pp. 559-590

[Google Scholar](#)

[Jessmer and Anderson, 2001](#) S.L. Jessmer, D. Anderson

The effect of politeness and grammar on user perceptions of electronic mail

North Am. J. Psychol., 3 (2) (2001), pp. 331-346

[View Record in Scopus](#) [Google Scholar](#)

[Jex, 1988](#) H.R. Jex

Measuring mental workload: problems, progress, and promises

P.A. Hancock, N. Meshkati (Eds.), Human Mental Workload, Elsevier Science Publishers B.V., Amsterdam, Netherlands (1988), pp. 3-39

[Google Scholar](#)

[Jiang et al., 2000](#) J.J. Jiang, G. Klein, R.G. Vedder

Persuasive expert systems: the influence of confidence and discrepancy

Comput. Hum. Behav., 16 (2000), pp. 99-109

[Article Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Johnston et al., 2015](#) A.C. Johnston, M. Warkentin, M. Siponen

An enhanced fear appeal rhetorical framework: leveraging threats to human asset through sanctioning rhetoric

MIS Q., 39 (1) (2015), pp. 113-134

[View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Kaiser, 1974](#) H. Kaiser

An index of factor simplicity

Psychometrika, 39 (1) (1974), pp. 31-36

[Google Scholar](#)

[Kiesler and Sproull, 1992](#) S. Kiesler, L. Sproull

Group decision making and communication technology

Org. Behav. Hum. Decis. Process., 52 (1) (1992), pp. 96-123

[Article Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Kokini et al., 2012](#) C.M. Kokini, S. Lee, R.J. Koubek, S.K. Moon

Considering context: the role of mental workload and operator control in users' perceptions of usability

Int. J. Hum.-Comput. Interact., 28 (2012), pp. 543-559

[View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Lam, 2011](#) C. Lam

Linguistic politeness in student-team emails: its impact on trust between leaders and members

IEEE Trans. Prof. Commun., 54 (4) (2011), pp. 360-375

[View Record in Scopus](#) [Google Scholar](#)

[Lee et al., 2007](#) M.K.O Lee, C.M.K. Cheung, Z. Chen

Understanding user acceptance of multimedia messaging services: an empirical study

J. Am. Soc. Inf. Sci. Technol., 58 (13) (2007), pp. 2066-2077

[View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Lee et al., 2019](#) S. Lee, H. Rui, A.B. Whinston

Is best answer really the best answer? The politeness bias

MIS Q., 43 (2) (2019), pp. 579-600

[View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Leech's Politeness Principle \(Leech, 1983\)](#) Leech's Politeness Principle (Leech, 1983).

[Google Scholar](#)

[Leech 1983](#) Leech, G. (1983). Principles of Pragmatics. London, UK: Longman.

[Google Scholar](#)

[Leech, 2014](#) G. Leech

The Pragmatics of Politeness

Oxford University Press, New York, NY (2014)

[Google Scholar](#)

[Lengel and Daft, 1988](#) R.H. Lengel, R.L. Daft

The selection of communication media as an executive skill

Acad.Manag. Execut., 8 (2) (1988), pp. 225-232

[Google Scholar](#)

[Levy and Gvili, 2015](#) S. Levy, Y. Gvili

How credible is e-word of mouth across digital-marketing channels? the roles of social capital, information richness, and interactivity

J. Advertis. Res., 55 (1) (2015), pp. 95-109

[View Record in Scopus](#) [Google Scholar](#)

[Locher, 2004](#) M.A. Locher

Power and Politeness in Action: Disagreements in Oral Communication

Mouton de Gruyter, Berlin, Germany (2004)

[Google Scholar](#)

[Locher and Bousfield, 2008](#) M.A. Locher, D. Bousfield

Impoliteness in Language: Studies on its Interplay with Power in Theory and Practice

Mouton de Gruyter, Berlin, Germany (2008)

[Google Scholar](#)

[Lowry et al., 2006](#) P.B. Lowry, T.L. Roberts, N.C. Romano, P.D. Cheney, R.T. Hightower

The impact of group size and social presence on small-group communication: does computer-mediated communication make a difference

Small Group Res., 37 (6) (2006), pp. 631-661

[View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Mackiewicz, 2004](#) J. Mackiewicz

The effects of tutor expertise in engineering writing: a linguistic analysis of writing tutors' comments

IEEE Trans. Prof. Commun., 47 (4) (2004), pp. 316-328

[View Record in Scopus](#) [Google Scholar](#)

[Mackiewicz and Riley, 2003](#) J.M. Mackiewicz, K. Riley

The technical editor as a diplomat: linguistic strategies for balancing clarity and politeness

Tech. Commun., 50 (1) (2003), pp. 83-94

[View Record in Scopus](#) [Google Scholar](#)

[Maity et al., 2018](#) M. Maity, M. Dass, P. Kumar

The impact of media richness on consumer information search and choice

J. Bus. Res., 87 (2018), pp. 36-45

[Article Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Matteson, 2018](#) Matteson, S. (2018). How to protect your organization against 5 common browser security threats. Retrieved May 31, 2020 from

<https://www.techrepublic.com/article/how-to-protect-your-organization-against-5-common-browser-security-threats/>.

[Google Scholar](#)

[Mayer and Moreno, 1988](#) R.E. Mayer, R. Moreno

A split-attention effect in multimedia learning: evidence for dual processing systems in working memory

J. Educ. Psychol., 90 (2) (1988), pp. 312-320

[Google Scholar](#)

[McAfee 2017](#) McAfee. (2017). Grand Theft Data: Data Exfiltration Study: Actors, Tactics, and Detection. Retrieved May 28, 2020 from

<https://www.mcafee.com/enterprise/en-us/assets/reports/rp-data-exfiltration.pdf>.

[Google Scholar](#)

[McCroskey and Teven, 1999](#) J.C. McCroskey, J.J. Teven

Goodwill: a reexamination of the construct and its measurement

Commun. Monograph., 66 (1) (1999), pp. 90-103

[View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[McGinnies, 1973](#) E. McGinnies

Initial attitude, source credibility, and involvement as factors of persuasion

J. Exp. Soc. Psychol., 9 (1973), pp. 285-296

[Article](#) [Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Miller et al., 2008](#) C.A. Miller, P. Wu, H.B. Funk

A computational approach to etiquette: operationalizing brown and levinson's politeness model

IEEE Intell. Syst., 23 (4) (2008), pp. 28-35

[View Record in Scopus](#) [Google Scholar](#)

[Moody et al., 2018](#) G.D. Moody, M. Siponen, S. Pahnla

Toward a unified model of information security policy compliance

MIS Q., 42 (1) (2018), pp. 285-311

[View Record in Scopus](#) [Google Scholar](#)

[Moore, 1992](#) P. Moore

When politeness is fatal: technical communication and the “challenger” accident

J. Bus. Tech. Commun., 6 (3) (1992), pp. 269-292

[View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Morgan and Hancock, 2011](#) J.F. Morgan, P.A. Hancock

The effect of prior task loading on mental workload: an example of hysteresis in driving

Hum. Fact., 53 (1) (2011), pp. 75-86

[View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Myers, 1991](#) G. Myers

Politeness and certainty: the language of collaboration in an AI project

Soc. Stud. Sci., 21 (1) (1991), pp. 37-73

[_View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Nass et al., 1999](#) C. Nass, Y. Moon, P. Carney

Are people polite to computers? responses to computer-based interviewing systems

J. Appl. Soc. Psychol., 29 (5) (1999), pp. 1093-1110

[_View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[O'Donnell and Eggemeier, 1986](#) R.D. O'Donnell, F.T. Eggemeier

Workload assessment methodology

K. Boff, L. Kaufman, J. Thomas (Eds.), Handbook of Perception and Performance, Vol II, Wiley Interscience, New York, NY (1986)

42-1-42-9

[Google Scholar](#)

[Paglieri et al., 2014](#) F. Paglieri, C. Castelfranchi, C. da Costa Pereira, R. Falcone, A. Tettamanzi, S. Villata

Trusting the messenger because of the message: feedback dynamics from information quality to source evaluation

Comput. Math. Org. Theory, 20 (2) (2014), pp. 176-194

[View Record in Scopus](#) [Google Scholar](#)

[Park, 2008](#) J. Park

Linguistic politeness and face-work in computer mediated communication, part 2: an application of the theoretical framework

J. Am. Soc. Inf. Sci. Technol., 59 (14) (2008), pp. 2199-2209

[_View PDF](#)

[CrossRef](#)[View Record in Scopus](#)[Google Scholar](#)

[Pelletier and Sharp, 2008](#) L.G. Pelletier, E. Sharp

Persuasive communication and proenvironmental behaviours: how message tailoring and message framing can improve the integration of behaviours through self-determined motivation

Canad. Psychol., 49 (3) (2008), pp. 210-217

[_View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Petter et al., 2007](#) S. Petter, D. Straub, A. Rai

Specifying formative constructs in information systems research

MIS Q., 31 (4) (2007), pp. 623-656

[_View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Puhakainen and Siponen, 2010](#) P. Puhakainen, M. Siponen

Improving employees' compliance through information systems security training: an action research study

MIS Q., 34 (4) (2010), pp. 757-778

[View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Rieh and Danielson, 2008](#) S.Y. Rieh, D.R. Danielson

Credibility: a multidisciplinary framework

Ann. Rev. Inf. Sci. Technol., 41 (1) (2008), pp. 307-364

[Google Scholar](#)

[Riley, 2003](#) K. Riley

About face: comparing positive politeness in dummies and conventional software documentation

IEEE International Professional Communication Conference (IPCC) 2003 Proceedings (2003), pp. 1-12

[Google Scholar](#)

[Riley and Mackiewicz, 2003](#) K. Riley, J.M. Mackiewicz

Resolving the directness dilemma in document review sessions with non-native speakers

IEEE Trans. Prof. Commun., 46 (1) (2003), pp. 1-16

[View Record in Scopus](#) [Google Scholar](#)

[Ringle et al., 2015](#) Ringle, Christian M., Wende, Sven, & Becker, Jan-Michael. (2015).

SmartPLS 3. Bönningstedt: SmartPLS. Retrieved from <http://www.smartpls.com>.

[Google Scholar](#)

[Rissman and Rissman, 1987](#) R. Rissman, B.Z. Rissman

Compliance: i. noncompliance: a review ii. facilitating compliance

Fam. Syst. Med., 5 (4) (1987), pp. 446-467

[View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Rogers and Lee-Wong, 2003](#) P.S. Rogers, S.M. Lee-Wong

Re-conceptualizing politeness to accommodate dynamic tensions in subordinate-to-superior reporting

Journal of Bus. Tech. Commun., 17 (4) (2003), pp. 379-412

[View Record in Scopus](#) [Google Scholar](#)

[Sarstedt et al., 2011](#) M. Sarstedt, J. Henseler, C.M. Ringle

Multigroup analysis in partial least squares (PLS) path modeling: alternative methods and empirical result

Adv. Int. Market., 22 (1) (2011), pp. 195-218

[Google Scholar](#)

[Schick et al., 1990](#) A.G. Schick, L.A. Gorden, S. Haka
Information overload: a temporal approach
Account. Org. Soc., 15 (1990), pp. 199-220
[Article](#) [Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Schneider, 1987](#) S.C. Schneider
Information overload: causes and consequences
Hum. Syst. Manag., 7 (1987), pp. 143-153
[View PDF](#)
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Shaw et al., 2009](#) R.S. Shaw, C.C. Chen, A.L. Harris, H.J. Huang
The impact of information richness on information security awareness training effectiveness
Comput. Educ., 52 (2009), pp. 92-100
[Article](#) [Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Shaw et al., 2009](#) R. Shaw S., C. Chen C., A. Harris L., H. Huang J.
The Impact of Information Richness on Information Security Awareness Training Effectiveness
Comput. Educ., 52 (2009), pp. 92-100, [10.1016/j.compedu.2008.06.011](#)
[Article](#) [Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Short et al., 1976](#) J. Short, E. Williams, B. Christie
The Social Psychology Of Telecommunications
John Wiley, New York, NY (1976)
[Google Scholar](#)

[Shropshire et al., 2010](#) J. Shropshire, M. Warkentin, A.C. Johnston
Impact of negative message framing on security adoption
J. Comput. Inf. Syst., 51 (1) (2010), pp. 41-51
[View Record in Scopus](#) [Google Scholar](#)

[Sias et al., 2012](#) P.M. Sias, E.B. Gallagher, I. Kopaneva, H. Pedersen
Maintaining workplace friendships: perceived politeness and predictors of maintenance tactic choice
Commun. Res., 39 (2) (2012), pp. 239-268
[View PDF](#)
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Sproull and Kiesler, 1986](#) L. Sproull, S. Kiesler
Reducing social context cues: electronic mail in organizational communication
Manag. Sci., 32 (11) (1986), pp. 1492-1512
[View PDF](#)
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Stephan et al., 2010](#) E. Stephan, N. Liberman, Y. Trope

Politeness and psychological distance: a construal level perspective

J. Personal. Soc. Psychol., 98 (2) (2010), pp. 268-280

[_View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Sternthal et al., 1978](#) B. Sternthal, R. Dholakia, C. Leavitt

The persuasive effect of source credibility: tests of cognitive response

J. Consum. Res., 4 (1978), pp. 252-260

[View Record in Scopus](#) [Google Scholar](#)

[Teven, 2008](#) J.J. Teven

An examination of perceived credibility of the 2008 presidential candidates: relationships with believability, likeability, and deceptiveness

Hum. Commun., 11 (4) (2008), pp. 383-400

[Google Scholar](#)

[Teven and McCroskey, 1997](#) J.J. Teven, J.C. McCroskey

The relationship of perceived teacher caring with student learning and teacher evaluation

Commun. Educ., 46 (1997), pp. 1-9

[_View PDF](#)

[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[The One Brief, 2020](#) The One Brief. (n.d.)The key to a holistic cyber security program: the human element. Retrieved 5/28/2020 from

<https://theonebrief.com/people-humans-cyber-greatest-risks/>.

[Google Scholar](#)

[Trevino et al., 1990](#) L.K. Trevino, R.L. Daft, R.H. Lengel

Understanding managers' media choices: a symbolic interactionist perspective

J. Fulk, W. Steinfeld (Eds.), Organizations and Communication

Technology, Sage, Newbury Park, CA (1990), pp. 71-94

[_View PDF](#)

[CrossRef](#) [Google Scholar](#)

[Vergaro, 2002](#) C. Vergaro

“Dear sirs, what would you do if you were in our position?”. Discourse strategies in Italian and English monday chasing letters

J. Pragm., 34 (9) (2002), pp. 1211-1233

[Article Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Vinagre, 2008](#) M. Vinagre

Politeness strategies in collaborative e-mail exchanges

Comput. Educ., 50 (3) (2008), pp. 1022-1036

[Article Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Wästlund et al., 2008](#) E. Wästlund, T. Norlander, T. Archer
The effect of page layout on mental workload: a dual-task experiment
Comput. Hum. Behav., 24 (3) (2008), pp. 1229-1245
[Article Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Watts, 2003](#) R.J. Watts
Politeness
Cambridge University Press, Cambridge, UK (2003)
[Google Scholar](#)

[Watts et al., 1992](#) R.J. Watts, S. Ide, K. Ehlich
Trends in Linguistics, Studies and Monographs 59: Politeness in Language: Studies in its History, Theory, and Practice
Mouton de Gruyter, Berlin, Germany (1992)
[Google Scholar](#)

[Whitworth, 2005](#) B. Whitworth
Polite computing
Behav. Inf. Technol., 24 (5) (2005), pp. 353-363
[View PDF](#)
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Wiebe et al., 2010](#) E.N. Wiebe, E. Roberts, T.S. Behrend
An examination of two mental workload measurement approaches to understanding multimedia learning
Comput. Hum. Behav., 26 (3) (2010), pp. 474-481
[Article Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Yan et al., 2019](#) S. Yan, Y. Wei, C.C. Tran
Evaluation and prediction mental workload in user interface of maritime operations using eye response
Int. J. Ind. Ergonom., 71 (2019), pp. 117-127
[Article Download PDF](#) [View Record in Scopus](#) [Google Scholar](#)

[Yang et al., 2012](#) J. Yang, W. Kim, N. Amblee, J. Jeong
The heterogeneous effect of WOM on product sales: why is the effect of WOM valence mixed
Eur. J. Market., 46 (11/12) (2012), pp. 1523-1538
[View PDF](#)
[CrossRef](#) [View Record in Scopus](#) [Google Scholar](#)

[Zhang, 2013](#) Y. Zhang
The politeness principles in business negotiation
Cross-Cult. Commun., 9 (4) (2013), pp. 50-56
[Google Scholar](#)

Deanna House is an Assistant Professor, Information Systems and Quantitative Analysis at the University of Nebraska at Omaha. Her research interests are related to the behavioral aspects of cybersecurity and the protective and preventative measures performed by users and organizations. Deanna has recently published in journals such as *Behaviour and Information Technology*, *Journal of Information Technology Case and Application Research* and *Applied Economics* and presented at conferences such as *ICIS*, *AMCIS*, *Southern AIS*, and *The Lilly Conference*.

Gabriel Giordano is Associate Professor and chair of Analytics and Information Systems in the College of Business at Ohio University. His research looks at challenges with using new types of communication in organizations, detection of deception in computer-mediated communication, and implementation strategies for transformational enterprise systems. He has published in outlets such as *MISQ*, *Communications of the AIS*, *Journal of the AIS*, and *Communications of the ACM*.